

STANDARDS AND PROCEDURES			ARIZONA DEPARTMENT OF ADMINISTRATION	IT DIVISIONS (ISD & ITSD)
Section:	06	Title:	Information Security	
Sub Section:	03	Title:	Information Security	
Document:	01	Title:	Information Access	

1. STANDARD

The authority to read, write, modify, update, or delete information from ISD controlled automated files, data bases, or software will be established by the State designated Stewards of the information.

1.1. Summary of Standard Changes

01/23/02 – Revision 001 – 4. Section 4 'PROCESSING DEPARTMENT OF REVENUE INFORMATION' added to document.

1.2. Purpose

ISD Security will ensure that legitimate users of ISD computer systems or their products cannot access software or data unless they have been authorized to do so ensuring software and data integrity through the use of access controls which will identify all legitimate users and their access authority.

1.3. Scope

Policy applies to any internal or external customer or user of any ISD computer system or product.

1.4. Responsibilities

Information Stewards will dictate all access requirements concerning their information.

The ISD ISS Manager will act in a consultant role helping the Information Stewards to determine threats and procedures to combat those threats. They will formulate procedures in compliance with these procedures and State control mandates.

ISD ISS Security Specialists will strictly follow the access procedures as determined by the Information Steward and ISD ISS.

All ISD internal and external customers will strictly follow all access procedures as they apply to them.

1.5. Definitions and Abbreviations

1.6. Description of Standard

Statement of authority to use information on ISD computer systems. An Information Steward, designated by the State, is responsible for identifying all others who may access or transact upon their information. The Steward is responsible for setting the level of access (read, write, modify, update, delete, etc.) the user may have, and for seeing to it that their users follow the password and password protection policies required by ISD. Access rights will be documented in an Information Sharing Agreement created with the assistance of

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)
Section:	06	Title: Information Security
Sub Section:	03	Title: Information Security
Document:	01	Title: Information Access

ISD. Any changes to this Sharing Agreement will be made by the Steward, or his/her designee.

1.7. Implications

A designated Steward of Information must be identified, and have authority to make decisions concerning the information.

The designated Steward of information must identify who may have access to any type of such information.

ISD ISS must maintain controls that ensure that the dictates of their customers are followed.

Information Stewards will insure that users comply with ISD Security Function policy as it applies to passwords and password protection.

1.8. References

Section 6 (ISD Security), Sub Section 1 (General Policy), Document 2 (Information Ownership)
Sample Customer Sharing Agreement
ISD Access Control Form

1.9. Attachments

2. STEWARD INFORMATION SHARING AGREEMENT PROCEDURES

Designated Information Stewards in conjunction with ISD ISS will create an Information Sharing Agreement documenting who the Steward authorizes access to information and at what levels. The document will list who will have authority (Steward, or Steward designee) to make changes to the document.

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. Authorized Information Steward will be identified by the State as owners of the information.

2.2.2. The Information Steward, in conjunction with the ISD ISS Manager, or his/her designees, will create an Information Sharing Agreement (using the ISD Information Sharing Agreement standard format) which creates an Access List that identifies who can access the data, at what levels, and who has authority to make changes to this Access List.

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)
Section:	06	Title: Information Security
Sub Section:	03	Title: Information Security
Document:	01	Title: Information Access

2.2.3. The Information Steward will be responsible to see that all users on the access list comply with ISD Security Function policy as it applies to passwords and password protection.

2.2.4. ISD ISS Security Specialists will create access protocols using User ID's and password what comply with the Information Sharing Agreement and ISD Security Function policy. They will make necessary changes when requested by the authorized agent.

2.3. References

Sample Customer Sharing Agreement
ISD Access Control Form

2.4. Attachments

3. PROCESS ACCESS REQUESTS PROCEDURES

Upon receipt of a request authorized by the information Steward to modify access to information, an ISD Security Administrator will process the request.

3.1. Summary of Procedure Changes

3.2. Procedure Details

Upon receipt of a properly documented ISD Access Control Form, and after authentication, an ISD Security Administrator will process the request following procedures as stated in the 'ISD Restricted Security Procedures Manual'.

3.3. References

ISD Restricted Security Procedures Manual

3.4. Attachments

4. PROCESSING DEPARTMENT OF REVENUE INFORMATION

ISD will comply will all DOR and Federal IRS rules and regulations concerning access to Federal IRS information.

4.1. Summary of Procedure Changes

1/23/02 – Revision 001 – 4. This section added for New Procedure due to data center consolidations

4.2. Procedure Details

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)
Section:	06	Title: Information Security
Sub Section:	03	Title: Information Security
Document:	01	Title: Information Access

ISD will make available all employees designated by DOR requiring specialized information security training. Employees will sign any specialized forms or statements required for the access to Federal IRS information.

4.3. References

4.4. Attachments